MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 2,2016/2017

TSC7011 – SECURITY IN COMPUTING

(All sections / Groups)

11 FEBRUARY 2017
09.00 am - 12.00 pm
(3 Hours)

INSTRUCTIONS TO STUDENTS

1. This Question paper consists of **SEVEN pages (excluding this page)** with **FIVE Questions**.
2. Attempt **FOUR** out of **FIVE** questions. Each question carries 20 marks and the maximum mark allocated is **80**. The distribution of the marks for each question is given.
3. Please write all your answers in the Answer Booklet provided.

QUESTION 1:

a. For **each** of the **security attacks** given below,
   - Traffic analysis
   - Masquerade
   - Denial of Service (DOS)
   - Repudiation

   (i) Give a brief description **(4×1=4 marks)**
   (ii) Specify the category (passive or active) **(4×0.5=2 marks)**
   (iii) Specify the security goal threatened (confidentiality or integrity or availability) **(4×0.5=2 marks)**
   (iv) Give an example. **(4×1=4 marks)**

b. Explain the essential elements of a **symmetric encryption scheme** with the help of a diagram. **(4 marks)**

c. State any TWO differences between Steganography and Cryptography. **(2 marks)**

d. State any TWO differences between Unconditionally Secure Cipher and a Computationally Secure Cipher. **(2 marks)**

QUESTION 2:

a. One way to classify the malware is based on insider and outsider attacks.
   (i) Briefly explain what is meant by **'insider attacks'** and why it is considered as dangerous malware?
   (ii) Give any TWO examples of insider attacks with brief explanation.
   (iii) State any FOUR defence measures that can be taken against 'insider attacks'.

   (3×2=6 marks)

b. State what is meant by **'Trojan Horse'** and how it is different from 'virus'? **(2 marks)**

c. State the FOUR different ways that can be used by a **computer worm** to access a remote system. **(2 marks)**

d. State any FOUR reasons on the **importance of securing databases**. **(4 marks)**

e. (i) State what you mean by **"inference"** in relation to database security.
   (ii) State and briefly explain the TWO approaches that can be used for **"inference prevention"** for a statistical database.

   (2+4=6 marks)

Continued...

QUESTION 3:

a. State the **difference** between **Monoalphabetic and Polyalphabetic Ciphers** with two examples for each. **(4 marks)**

b. Assume that plaintext and ciphertext characters are represented as numerical values in Z_{26} as follows:

Plaintext →	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext →	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Answer the following questions:

(i) Assume the usage of **Affine Cipher**. Decrypt the following ciphertext with $\mathbf{k_1=7}$ and $\mathbf{k_2=6}$ in **modulus 26**, where the key k_1 is used with multiplicative cipher and the key k_2 is used with additive cipher.

RAN **(3 marks)**

(ii) Assume the usage of **Vigenère Cipher.** Encrypt the plaintext message "hardwork rewards" using the 4-character keyword "BEST". Ignore the spaces between the words. **(3 marks)**

Continued…

c. For **Data Encryption Standard (DES)**, answer the following questions with respect to the first round.

Assume that the **32-bit Right Half (R_0)** obtained after passing the plaintext through the Initial Permutation Table is given as

$$R_0 = (0100\ \ 1111\ \ 1010\ \ 0101\ \ 0110\ \ 1111\ \ 1101\ \ 0101)_2$$

Assume also that the **48-bit first round sub-key (K_1)**, produced after passing the 64-bit key through Permuted Choice One (PC-1), left circular shift and Permuted Choice Two (PC-2), is given as

$$K_1 = (110001\ \ 100010\ \ 010111\ \ 110011\ \ 100111\ \ 100110\ \ 000000\ \ 010011)_2$$

(i) Expand R_0 using the following Expansion Permutation (E) Table to get **48-bit E [R_0]**. **(4 marks)**

Expansion Permutation (E) Table

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

(ii) Calculate $A = E[R_0] \oplus K_1$ using the 48-bit result obtained in (i) and the given 48-bit first round sub-key. **(2 marks)**

(iii) Group the 48-bit result **(A)** obtained in (ii) into sets of 6 bits and evaluate the corresponding S-box substitutions (S_1 and S_2) for the first two sets of 6 bits to produce **4-bit output each**. **(2+2=4 marks)**

Definition of DES S-Boxes

S_1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

Continued...

QUESTION 4:

a. (i) Draw the diagram for encryption for **Cipher Feedback Mode** if the size of plaintext block (r) is equal to the size of the block used in block cipher (n). **(2 marks)**

(ii) Consider the usage of **ciphertext stealing technique** for **Electronic Code Book mode**. Show the diagram for encryption and decryption for the last two blocks. **(4 marks)**

b. With the help of Block diagram, briefly explain how a **Public Cryptosystem** can be used to provide **authentication** using the encryption with private key. **(4 marks)**

c. With reference to **Rivest-Shamir-Adleman (RSA)** cryptosystem, answer the following:

(i) Identify the **public key {e,n} and private key {d,n}** for the following data using RSA_Key_Generation algorithm given below. **(4 marks)**

p=7; q=11; e=17

where

p and q are two prime numbers

e is an integer with gcd (ϕ (n) , e) =1; 1 < e < ϕ (n);

RSA_Key_Generation

{

Select two large primes p and q such that $p \neq q$.

$n \leftarrow p \times q$

$\phi(n) \leftarrow (p-1) \times (q-1)$

Select e such that $1 < e < \phi(n)$ and e is coprime to $\phi(n)$

$d \leftarrow e^{-1} \bmod \phi(n)$ // d is inverse of e modulo $\phi(n)$

Public_key $\leftarrow$ (e, n) // To be announced publicly

Private_key $\leftarrow d$ // To be kept secret

return Public_key and Private_key

}

Continued...

(ii) With the help of the following algorithms, perform **encryption and decryption** using the keys derived in (i) and using the plaintext message **P=8.** **(6 marks)**

```
RSA_Encryption (P, e, n)                  // P is the plaintext in Z_n and P < n
{
   C ← Fast_Exponentiation (P, e, n)      // Calculation of (P^e mod n)
   return C
}
```

```
RSA_Decryption (C, d, n)                  //C is the ciphertext in Z_n
{
   P ← Fast_Exponentiation (C, d, n)      // Calculation of (C^d mod n)
   return P
}
```

```
Square_and_Multiply (a, x, n)
{
    y ← 1
    for (i ← 0 to n_b − 1)                // n_b is the number of bits in x
    {
        if (x_i = 1)   y ← a × y  mod n   // multiply only if the bit is 1
        a ← a^2 mod n                     // squaring is not needed in the last iteration
    }
    return y
}
```

Continued…

QUESTION 5:

a. Multipurpose Internet Mail Extension (MIME) is an extension to the old RFC 822 specification of an Internet mail format and S/MIME is a security enhancement to the MIME Internet e-mail format standard, based on technology from RSA Data Security. Answer the following with respect to the above protocol.

(i) State the purpose of using MIME as an extension protocol to Internet mail. **(1 mark)**

(ii) Assuming the usage of **quoted-printable** scheme for performing content-Transfer-Encoding in S/MIME protocol, perform the encoding of the following binary data.

10000011 01010010 00110011 10100110

Identify the **equivalent codes** based on the following ASCII table. **(4 marks)**

The Standard ASCII Table

ASCII Character	Dec	Hex	ASCII Character	Dec	Hex	ASCII Character	Dec	Hex	ASCII Character	Dec	Hex
nul	0	00	space	32	20	@	64	40	`	96	60
soh	1	01	!	33	21	A	65	41	a	97	61
stx	2	02	"	34	22	B	66	42	b	98	62
etx	3	03	#	35	23	C	67	43	c	99	63
eot	4	04	$	36	24	D	68	44	d	100	64
enq	5	05	%	37	25	E	69	45	e	101	65
ack	6	06	&	38	26	F	70	46	f	102	66
bell	7	07	'	39	27	G	71	47	g	103	67
backspace	8	08	(	40	28	H	72	48	h	104	68
horiztab	9	09	)	41	29	I	73	49	i	105	69
linefeed	10	0A	*	42	2A	J	74	4A	j	106	6A
verticaltab	11	0B	+	43	2B	K	75	4B	k	107	6B
formfeed	12	0C	,	44	2C	L	76	4C	l	108	6C
cr	13	0D	-	45	2D	M	77	4D	m	109	6D
so	14	0E	.	46	2E	N	78	4E	n	110	6E
si	15	0F	/	47	2F	O	79	4F	o	111	6F
dle	16	10	0	48	30	P	80	50	p	112	70
dc1	17	11	1	49	31	Q	81	51	q	113	71
dc2	18	12	2	50	32	R	82	52	r	114	72
dc3	19	13	3	51	33	S	83	53	s	115	73
dc4	20	14	4	52	34	T	84	54	t	116	74
nak	21	15	5	53	35	U	85	55	u	117	75
syn	22	16	6	54	36	V	86	56	v	118	76
etb	23	17	7	55	37	W	87	57	w	119	77
can	24	18	8	56	38	X	88	58	x	120	78
em	25	19	9	57	39	Y	89	59	v	121	79
sub	26	1A	:	58	3A	Z	90	5A	z	122	7A
esc	27	1B	;	59	3B	[	91	5B	{	123	7B
fs	28	1C	<	60	3C	\	92	5C	|	124	7C
gs	29	1D	=	61	3D	]	93	5D	}	125	7D
rs	30	1E	>	62	3E	^	94	5E	~	126	7E
us	31	1F	?	63	3F	_	95	5F	delete	127	7F

Continued...

(iii) State the steps involved in the process of creating an object of **Enveloped-Data Content Type** for providing privacy for the message using S/MIME protocol.

(2 marks)

b. The **Secure Electronic Transaction (SET)** is an open encryption and security specification that is designed for protecting credit card transactions on the Internet. State the steps involved in SET for hiding the credit card details of the cardholder from the merchant. **(3 marks)**

c. The **black list** and the **white list** approaches are the two fundamental approaches to create **firewall policies** to effectively minimize vulnerability to the outside world while maintaining the desired functionality for the machines in the trusted internal network. State the major difference between these two approaches.

(2 marks)

d. Once the operating system is appropriately built, secured, and deployed, the process of maintaining security results from the constantly changing environment, the discovery of new vulnerabilities, and hence exposure to new threats. State any FOUR additional steps involved in the **process of operating system security maintenance**. **(2 marks)**

e. Security designers develop formal models of computer security that can be used to verify security designs and implementations. The Bell-LaPadula (BLP) is one such model that deals with confidentiality. State the FOUR **access modes** defined by this **BLP model**. **(2 marks)**

f. State and briefly explain any **FOUR security threats** to **wireless networks.**

(4 marks)

End of questions